Testimony by Jeffrey I. Schiller,
Network Manager/Security Architect,
Massachusetts Institute of Technology,
before the
House Committee on Government Reform
(as prepared for delivery)

May 15, 2003

My name is Jeff Schiller and I am the Network Manager at the Massachusetts Institute of Technology. I have had this position since 1984. I have been involved in the development and operation of the Internet from its very early history. I am also a security expert, an author of the MIT Kerberos Authentication System, which is used as the basis for authentication in Windows 2000 and Windows XP, among other systems. I have also deployed a Public Key Infrastructure at MIT that has been operating since 1996. This infrastructure provides for secure web authentication and authorization at MIT.

From 1994 through 2003 I served as one of the two Area Directors for Security for the Internet Engineering Task Force, the Standards body of the Internet. In this role I was responsible for the groups working on security protocols for the Internet as well as for reviewing all Internet Standards documents for correctness. I am therefore very familiar with the protocol workings of the Internet as well.

I am here today to help you look at what are called "Peer to Peer" file sharing programs, through the lens of security.

It is funny how we refer to these programs as "Peer to Peer" when the architecture of the Internet itself is peer to peer. E-mail is peer to peer, even web browsing is peer to peer. Most people don't run a web server, however the Internet would work just fine if they did. The innovative nature of the Internet itself is dependent on this peer to peer nature. If it were not that way, E-mail may have never arisen as the important application that it is. In fact I remember the days when E-mail was considered a waste of network resources and quasi forbidden, yet today it is one of the killer applications of the Internet. If it were not for the peer to peer nature of the Internet, a programmer at CERN in Switzerland could not have modernized the CERN telephone directory, and invented the World Wide Web as a side effect!

So what are we really talking about here today. What makes the programs we are concerned about different from those that preceded them?

The key attributes of what we call peer to peer programs are:

- Storage of files on "client" computers, desktops and laptops. Typically not computers that we view as "servers" more traditionally used to store data.
- The organization of networks of computers all which use the same file sharing network. When you start up a peer to peer file sharing program, it "joins" the network of other people already running the program. This "joining" takes the form of

making a direct Internet connection to one or more other computers running the same program.

- The ability of one computer user to request a file by name or attribute and have a listing of available copies downloaded to that computer. The user can then select and download the data file itself.

So are these programs secure? Well, we have to ask: "Compared to What?"

In some ways they are more secure then E-mail. Whereas E-mail tends to be "pushed" to you, file sharing is more like web browsing, you have to go looking for information, it doesn't show up on your computer unbidden.

So what are the risks to the end-user of a file sharing program?

A malicious person might place a file in the network with the name of a popular download, but instead of providing the information advertised, the file contains a virus or other active content that when opened results in compromise or damage to the end-user's computer. One might argue that this risk is present in web browsing as well. We have heard of plenty of cases of security weaknesses in web browsers that start with the phrase "A malicious user could put content on their webpage that..."

However when web browsing, people have some sense of where they are going (at least some people do!). File sharing programs tend to hide this level of detail. Instead they will show you a menu of several places where the file you request is located, listing each by Internet address, which isn't particularly meaningful to someone.

My conclusion is simply this: File sharing programs, as viewed by the end-user are no more or less secure then other common Internet applications such as web browsing or reading E-mail. The exact technical details are slightly different. The risks are slightly different, but the magnitude of danger is about the same.

So where do these program really deviate, if not now, in the future?

To go further we need to stop for a second and talk about the various actors involved in the use of a computer. Up until now I have discussed the world from the view of an end-user, the user of a client computer either at home or in an office.

However there are four different "actors" potentially involved. The end-user is one obvious actor. The provider of the file being requested is another actor. The owner of the computer or enterprise the computer is located in, is an actor with a stake in the security properties and risks of a file sharing program. Finally, there is the author of the file sharing program and the "operator" of the peer to peer file sharing network.

Unlike E-mail and Web Browsing, the peer to peer file sharing networks are still evolving. This means that the "author" of the programs are still active "actors" continuing to modify their programs to address both new features and to adapt to the operating environment of the Internet. It is this adaption that is cause for concern.

The administrator of an enterprise network, or the parent of a child who uses a computer. Can install programs and/or technology to attempt to control traditional Internet applications such as E-mail and Web Browsing and even newer applications such as on-line chat rooms. The authors of these more traditional applications do not evolve their programs with the goal of subverting these controls. Not so the peer to peer file sharing networks.

The authors of the peer to peer file sharing networks continue to modify and adapt their programs with the apparent goal, among others, of subverting attempts to control them. I cannot authoritatively speak as to why they wish to do this, you will have to ask them. However I know from my role as a network manager that many institutions wish to block or throttle[1] these programs either because of copyright concerns or because of the cost of providing the Internet bandwidth these applications consume.

Presumably this blocking or throttling is unpopular with the users of the file sharing programs and the authors are merely reacting to the demands of their customers!

It is worth noting that the institutions that have the most difficulty with controlling peer to peer file sharing programs are those that are completely open, or quasi open, such as universities. It is possible to completely firewall an enterprise so that file sharing programs cannot make connection across the firewall. This is accomplished by blocking all access between the internal "Intranet" and the Internet at large, and only allowing limited applications, through application level proxy programs, to cross the firewall.

However many institutions cannot enforce such a harsh policy. Research universities as a community need to permit their researchers more or less unfettered access to the Internet. It is through this access that innovation is fostered and new Internet applications are developed. In such organizations some protocols, such as E-mail or web browsing are controlled either in order to control costs, or to filter out junk E-mail. However most other protocols are permitted unimpeded. If we establish controls on the protocol ports[2] used by the peer to peer file sharing programs, the authors of those programs simply have the next version use a different port. It is also possible for them to switch ports continuously, making it difficult to track and to control.

So in conclusion, peer to peer file sharing technology is not fundamentally more or less secure then the common Internet applications that people use everyday. However the goals of the authors of these programs are, among others, to subvert controls placed on them by enterprises. As such they may permit inadvertent, or malicious compromise of those systems that an enterprise wishes to protect.

One final comment. I have been saying today that a major risk of peer to peer file sharing is that it attempts to subvert legitimate controls placed on its use. Considering the case where the controlling party is an institution or parent. However we do have to realize that sometimes the "controlling" party may be a government whose goal is to control their

1 Limit the Internet bandwidth consumed by.

2 Internet applications typically communicate over "ports" which are number assigned to the different protocols. These numbers are used by two computers communicating to label data as to what application it is for. For example E-mail travels over port 25 and most web browsing happens over port 80.

citizens access to the Internet at large. In such an environment peer to peer file sharing may well be an important way to bring freedom of expression to an otherwise oppressed population. It all depends on your point of view.

Thank you for inviting me here today and I hope I have provided information that you will find useful. I am available for any questions.